Finite Sets in Homotopy Type Theory

Dan Frumin  
Radboud University  
Institute for Computation and Information Sciences  
The Netherlands  
dfrumin@cs.ru.nl

Léon Gondelman  
Radboud University  
Institute for Computation and Information Sciences  
The Netherlands  
lgg@cs.ru.nl

Herman Geuvers  
Radboud University  
Institute for Computation and Information Sciences  
The Netherlands  
herman@cs.ru.nl

Niels van der Weide  
Radboud University  
Institute for Computation and Information Sciences  
The Netherlands  
nweide@cs.ru.nl

1 Introduction

We study finite sets and finite types from the point of view of homotopy type theory (HoTT). HoTT aims at providing a formal system that allows the user to reason about and compute with mathematical structures at the proper level of abstraction. To do so, it employs, for example, the univalence axiom and higher inductive types. Univalence allows treating isomorphic structures as equal and higher inductive types allow – among other things – reasoning inductively over structures modulo an equivalence relation. We apply these techniques to finite sets and finite types. HoTT should provide the proper computational mechanisms and reasoning principles for finite sets, like taking the union of two finite sets, counting the number of elements, having an element-of relation and extensional equality for sets.

In this paper we define the type of finite sets over a type \(A\) as a higher inductive type in two ways. First we define \(\mathcal{K}(A)\) (the type of Kuratowski-finite sets) as the free join semi-lattice over \(A\). We give the induction (and recursion) principle, show how some basic operations can be defined, and we show how some basic properties can be proved. Second we define \(\mathcal{L}(A)\) (the type of listed finite sets) as the higher inductive type of lists over \(A\) such that swapping elements and removing duplicates preserves equality. We show that these two types are equivalent.

This approach is inspired by topos theory [25] and it is translated to HoTT by encoding free algebras as higher inductive types [46]. These two views are connected since sets in HoTT form a predicative topos [40].

Our development of finite sets inside HoTT adequately stresses the subtlety of some of the defined functions: for example, to count the number of elements of a finite set, we need the underlying type \(A\) to have decidable mere equality (similarly for defining the intersection of two finite sets). That our type of finite sets is at the proper level of abstraction, is further exemplified by the fact that a naive “size function” that just takes the length of the list of elements can simply not be defined in our system. This is because such a naive size function does not preserve equality.
In intuitionistic mathematics there are essentially different ways of defining the “finite set”. The most well-known, due to Bishop [13], states that a set $A$ is finite if it is equivalent to a canonical finite set $\{0, \ldots, n\}$ for some $n \in \mathbb{N}$. Alternatively, we could consider “Kuratowski-finiteness”, which states that there is a Kuratowski-finite subset of $A$ that contains all inhabitants of type $A$. Yet another way of defining that $A$ is finite, is by saying that it can be enumerated: there is a list of objects of type $A$ that contains all $a : A$. We prove that the latter two notions (Kuratowski-finite and enumerated) are equivalent. Bishop-finiteness is really stronger as it implies that equality on the type $A$ is decidable. In the presence of decidable equality, all three notions coincide. Hence, the most general of these are Kuratowski-finiteness and enumeratedness.

In computer science, there are various concrete data structures for finite sets, for example lists, labeled binary trees, binary search trees, AVL trees, and so on. Using our higher inductive type $\mathcal{K}(A)$ of Kuratowski-finite sets, we define the notion of a “implementation of finite sets over $A$”, which is basically a type $T(A)$ with some operations satisfying some equational laws. More precisely, we define a signature and then $T(A)$ is an implementation of finite sets if $T(A)$ interprets that signature and we have a homomorphism from $T(A) \to \mathcal{K}(A)$. The aforementioned examples are all implementations of finite sets and so is $\mathcal{K}(A)$ itself. We show how a function defined on $\mathcal{K}(A)$ can be transferred to a function on another implementation of finite sets over $A$ while the properties are automatically preserved.

**Contributions** The paper is intended as a case study in HoTT and its contributions are the following.

- It presents the first consequent Coq development of finite sets using higher inductive types;
- It translates the notions of Kuratowski-finiteness and enumeratedness to HoTT in a proof-irrelevant way and it gives a formalized comparative study between these notions and Bishop-finiteness;
- It defines an interface of finite sets suitable for data refinement such that the implementations properties can automatically be deduced.

**Implementation** All results in the paper are formalized in Coq using the HoTT library [9]. The formalization can be found at [http://cs.ru.nl/~nweide/fssets/finite sets.html](http://cs.ru.nl/~nweide/fssets/finite sets.html) and contains many more results about finite sets and finite types. An overview of the results, linking definitions and theorems presented in this paper with formalized proofs, can be found in the file ‘CPP.v’. Our development contains 4051 lines of code of which 1406 are specifications and 2645 are proofs. To implement finite sets efficiently, we use type classes for overloading and proof automation [27, 43].

### 1.1 Homotopy Type Theory

We end this introduction with a short recap of homotopy type theory where we also fix some notations. Everything we describe is standard [46], so readers familiar with HoTT can skip this section.

In HoTT, a crucial role is played by the identity type, which is the inductive type with only one constructor, $\text{refl}$ of type $\prod (x : A), x = x$, and with the $J$-rule as eliminator. The $J$-rule says that given a type family $\varphi : \prod (x : A), x = y \to \text{Type}$ and an inhabitant $r$ of type $\prod (x : A), \varphi x x (\text{refl} x)$, we get

$$J(\varphi, r) : \prod (x, y : A), \prod (p : x = y), \varphi x y p.$$ 

In HoTT, a proof of an equality $p : a = b$ is interpreted as a “path” and from a computer science perspective, we may view the term $p$ as a way of transforming the object $a$ into the object $b$.

With the $J$-rule, we get $\text{symm}_A : \prod x, y : A, x = y = x$ and $\text{trans}_A : \prod x, y, z : A, x = y \to y = z \to x = z$ representing symmetry and transitivity of equality respectively. For paths $p : a = b$ and $q : b = c$ we write $p^{-1} := \text{symm}_A a b p$ and $p \cdot q := \text{trans}_A a b c p q$.

The $J$-rule also allows substituting paths along type families (Leibniz’ law). For $X$ and $Y$ types and $P : X \to \text{Type}$ a type family over $X$ we define

$$\text{transport} : \prod (x, y : X), x = y \to P x \to P y.$$ 

As usual, we abbreviate this to $p_\ast := \text{transport} x y p$.

Apart from the identity type, we also have definitional equality, which is not a judgment in the system but rather an equality that can be checked automatically by performing reductions. Definitional equality is denoted by $\equiv$. The conversion rule implies that definitionally equal types and terms cannot be distinguished: if $m : A$ and $B : \text{Type}$ such that we have $A \equiv B$, then $m : B$. For transport we have the definitional equality ($\text{refl} t) \equiv \text{refl} s$.

Frequently, we need to compare terms $s : P x$ and $t : P y$ in some type family $P : X \to \text{Type}$. If we have a path $q : x = y$, then we can compare $s$ and $t$ by transporting along $q$. More precisely, we define $s =_q t := (q, s) = t$.

Another major feature of homotopy type theory is the univalence axiom which roughly says that equivalent types are equal. With this axiom one can prove function extensionality. To formulate it more precisely, we first need to define equivalences. Two types $A$ and $B$ are equivalent if there is a map $f : A \to B$ such that $\text{isEquiv}(f)$ where

$$\text{isEquiv}(f) := \sum_{g : B \to A} (f \circ g = \text{id}_B) \times \sum_{h : B \to A} (h \circ f = \text{id}_A).$$

We write $A \simeq B := \sum f : A \to B \text{isEquiv}(f)$ and we call $f$ an equivalence. The univalence axiom asserts that equivalent types are equal meaning that there is an equivalence $\text{ua}$ from the equivalences $A \simeq B$ to the paths $A = B$.

HoTT also refines the propositions-as-types perspective via the notion of a *mere proposition*. A type $A$ is a mere
Finite Sets in Homotopy Type Theory

2 Definitions

Our goal is to define a type \( \mathcal{K}(A) \) representing the finite subsets of some type \( A \). In type theory and functional programming languages one defines data types using inductive types. However, such types are freely generated by constructors and that way equations on the type cannot be guaranteed. When defining finite subsets, that lack of equations becomes a serious hurdle.

With higher inductive types (HITs) this hurdle can be overcome. Since HITs allow both point and path constructors in their definitions, the type and its equality types are generated by the point and the path constructors respectively.

In this section we give two equivalent representations of finite sets in terms of higher inductive types. The first representation corresponds to the Kuratowski finite sets [29]. Here finite sets are built step by step starting with the empty set and singleton sets and then making larger sets by taking the union. In an abstracter language, the finite subsets of \( A \) form the free join semi-lattice on \( A \).

The second representation is based on finite lists. Intuitively, sets are given by a list of elements, but the order and multiplicity do not matter. This means that swapping two elements and removing duplicates in the list gives the same finite set.

2.1 Kuratowski Finite Sets

We start by defining the type \( \mathcal{K}(A) \) of finite subsets of \( A \).

**Definition 2.1.** Given a type \( A \), we define the type \( \mathcal{K}(A) \) of Kuratowski finite sets as follows.

\[
\begin{align*}
\text{Higher Inductive Type } \mathcal{K}(A) := \\
\{ \emptyset : \mathcal{K}(A) \\ \\ \{ \cdot \} : A \to \mathcal{K}(A) \\ \\ \cup : \mathcal{K}(A) \to \mathcal{K}(A) \to \mathcal{K}(A) \\ \\ \text{nl} : \bigcup \{ (x : \mathcal{K}(A)), \emptyset \cup x = x \} \\ \\ \text{nr} : \bigcup \{ (x : \mathcal{K}(A)), x \cup \emptyset = x \} \\ \\ \text{idem} : \bigcup \{ (x : A), \{ x \} \cup \{ x \} = \{ x \} \} \\ \\ \text{assoc} : \bigcup \{ (x, y, z : \mathcal{K}(A)), x \cup (y \cup z) = (x \cup y) \cup z \} \\ \\ \text{com} : \bigcup \{ (x, y : \mathcal{K}(A)), x \cup y = y \cup x \} \\ \\ \text{trunc} : \bigcup \{ (x, y : \mathcal{K}(A)), \{ (p, q : x = y), p = q \} \}
\end{align*}
\]

Every line introduces a new constructor of the higher inductive type \( \mathcal{K}(A) \). The first three lines correspond to the point constructors, and the other lines correspond to the path constructors. All of those paths, except for \( \text{trunc} \), are paths between points and they describe basic join semi-lattice laws such as associativity, commutativity, etc. Finally, the constructor \( \text{trunc} \), which is a path between paths, forces the higher groupoid \( \mathcal{K}(A) \) to be an \( hSet \).

Note that \( \text{nr} \) can be derived from \( \text{nl} \) and \( \text{com} \). Since the type is truncated, these two paths are the same. Hence, it does not matter whether we add just \( \text{nl} \) or both \( \text{nl} \) and \( \text{nr} \). We choose the latter, more symmetrical, option.
Now that we know how finite sets are generated by constructors, the next step is to equip the type $\mathcal{K}(A)$ with induction and recursion principles to describe how our finite sets can be used. Since the recursion principle can always be derived from the induction principle, we only give the latter one here.

**Definition 2.2.** Given a type family $\varphi : \mathcal{K}(A) \rightarrow \text{Type}$, the induction principle postulates that, provided how $\varphi$ acts on each of the constructors of $\mathcal{K}(A)$, an eliminator of type $\prod (x : \mathcal{K}(A)), \varphi x$ exists. Figure 1 shows the induction principle of $\mathcal{K}(A)$ in detail. For each constructor $C \in \{\varnothing, \ldots\}$, we denote by $C\varphi$ the action of $\varphi$ on $C$.

In addition, there are computation rules describing how the eliminator acts on each of the constructors. We will only need the computation rules for the points, and thus we will not give any computation rule for the path constructors. For the points we just use the same rules as for inductive types.

The path computation rules are not needed, since we only use induction to prove mere propositions, and, since all paths are equal in a proposition, we do not need to simplify paths with computation rules. Let us illustrate how induction works on the following example.

**Lemma 2.3 (Union-idem).** For any $x : \mathcal{K}(A), x \cup x = x$.

*Proof.* By induction on $x$. If $x = \varnothing$, the term $\text{nl} \varnothing$ has the expected type $\varnothing \cup \varnothing = \varnothing$. Similarly, if $x = \{a\}$, we directly get $\text{idem} a : \{a\} \cup \{a\} = \{a\}$. If $x = x_1 \cup x_2$ and $x_1 \cup x_2 = x_1$ for $i = 1, 2$, we need to show that the term $x_1 \cup x_2$ is equal to $(x_1 \cup x_2) \cup (x_1 \cup x_2)$. Using associativity and commutativity, we can show that the latter is equal to $(x_1 \cup x_1) \cup (x_2 \cup x_2)$ and applying induction hypotheses allows us to conclude this case.

It remains to construct images of the path constructors $\text{nl} \varphi, \text{nr} \varphi$, etc., where $\varphi x$ is equal to $x \cup x = x$. First note that it is easy to produce $\text{trunc} \varphi$ from $\text{trunc}$. Indeed, since $\mathcal{K}(A)$ is an hSet, $\varphi x$ is an hProp. Consequently, $\varphi x$ is an hProp [46, Lemma 3.3.4] which gives us $\text{trunc} \varphi$. In addition, we can construct each of remaining terms $\text{nl} \varphi, \text{nr} \varphi, \ldots$ straightforwardly using the fact that $\varphi x$ is an hProp, which allows us to conclude. $\square$

### 2.2 Extensionality

One of the important axioms of set theory is extensionality which says that two sets are equal if and only if they have the same elements. Since our higher inductive type $\mathcal{K}(A)$ represents finite sets, we show that it satisfies extensionality. Let us start by defining the membership function.

**Definition 2.4 (Membership).** Assume univalence. Given a type $A$, we construct by induction the membership function $\mathcal{E}$ of type $A \rightarrow \mathcal{K}(A) \rightarrow \text{hProp}$. For $a : A$ we define membership for the points as follows

- $a \in \varnothing \equiv \bot$,
- $a \in \{b\} \equiv ||a = b||$,
- $a \in (x_1 \cup x_2) \equiv a \in x_1 \lor a \in x_2$

where $B \lor C$ is defined by $||B \lor C||$. Dealing with other cases amounts to prove that (hProp, $\lor, \bot$) is a join semi-lattice. With univalence this is straightforward.

In the remainder we shall assume the univalence axiom unless stated otherwise. Note that we define membership here as a function into hProp and not into Bool. As we shall see in the next section, defining the latter is also possible, but requires assuming decidable mere equality on $A$. Let us now state the extensionality for $\mathcal{K}(A)$.

**Theorem 2.5 (Extensionality).** For all $x, y : \mathcal{K}(A)$ the types $x = y$ and $\prod (a : A), (a \in x = a \in y)$ are equivalent.

We prove this theorem via the following equivalences:

$x = y \equiv (y \cup x = x) \times (x \cup y = y) \equiv \prod_{a : A} a \in x = a \in y$.

Let us show only the following auxiliary lemma here.
Lemma 2.6. For all \( x, y : \mathcal{K}(A) \) we have
\[
\prod_{a : A} a \in y \rightarrow a \in x \rightarrow y \uplus x = x.
\]

Proof: We prove the result by induction over \( y \) keeping \( x \) as a free variable. More specifically, we construct for \( x : \mathcal{K}(A) \) a map of type
\[
\prod_{y : \mathcal{K}(A)} \prod_{a : A} a \in y \rightarrow a \in x \rightarrow y \uplus x = x.
\]

Note that it suffices to just consider the cases of the point constructors. Indeed, other cases are straightforward since for each \( y \) the resulting type is a mere proposition.

If \( y = \emptyset \), then \( \text{nil} \ x : \emptyset \uplus x = x \).

If \( y = \{b\} \) for some \( b : A \), we have the hypothesis \( H \) of type \( \prod_{a : A} a \in \{b\} \rightarrow a \in x \) and we need to show the equality \( \{b\} \uplus x = x \). To do so, we show that
\[
\prod_{x : \mathcal{K}(A), b \in x} b \in \{b\} \uplus x = x
\]
by induction on \( x \). Again it suffices to consider just the point constructors for the same reason as above.

If \( x = \emptyset \), we have \( b \in \emptyset \), which is a contradiction.

If \( x = \{c\} \), we have \( p' : b \in \{c\} \) and we need to show that \( \{b\} \uplus \{c\} = \{c\} \). Note that by Definition 2.4 we have that \( p' \) is of type \( \{b\} \uplus c \). Since the goal is a mere proposition, we get a path \( p : b = c \) by truncation recursion. Now we can define the desired path as follows
\[
\text{ap} \ (\lambda x, \{x\} \uplus \{c\}) \ p \ 	ext{idem} \ c : \{b\} \uplus \{c\} = \{c\}.
\]

Otherwise, we have \( x = x_1 \uplus x_2 \) and we have the hypothesis \( H' \) of type \( b \in x_1 \uplus x_2 \), and for \( i = 1, 2 \), the hypotheses
\[
H_i : b \in x_i \rightarrow \{b\} \uplus x_i = x_i.
\]

By definition, \( H' \) is of type \( b \in x_1 \uplus b \in x_2 \). Similarly to the previous case, we get by truncation recursion an inhabitant of type \( b \in x_1 \uplus b \in x_2 \). Hence, there are two cases to consider.

If \( t : b \in x_1 \), then we have the following chain of equalities
\[
\{b\} \uplus (x_1 \uplus x_2) = (\{b\} \uplus x_1) \uplus x_2 = x_1 \uplus x_2.
\]

The case \( t : b \in x_2 \) is proven similarly.

Lastly, if \( y = y_1 \uplus y_2 \) and if we have a term \( H \) of type \( \prod_{a : A} a \in y_1 \uplus y_2 \rightarrow a \in x \) and for \( i = 1, 2 \) hypotheses
\[
H_i : \prod_{a : A} a \in y_i \rightarrow a \in x \rightarrow y_i \uplus x = x,
\]
then we need to prove \( (y_1 \uplus y_2) \uplus x = x \). Using the induction hypotheses, we get paths \( p_1 : y_1 \uplus x = x \) and \( p_2 : y_2 \uplus x = x \) from which we get the desired path as the following chain of equalities
\[
(y_1 \uplus y_2) \uplus x = y_1 \uplus (y_2 \uplus x) = y_1 \uplus x = x \quad \Box.
\]

2.3 Listed Finite Sets

When working with finite sets, one would naturally expect to have standard operations such as size of a set. However, it quickly turns out that just using the higher inductive type \( \mathcal{K}(A) \) is problematic.

There are two issues. First of all, without being able to decide membership, it is impossible to define size (as we shall see in the next section). Second of all, even assuming decidable membership, we would get stuck when defining the size for the union. Indeed, the corresponding equation
\[
\#(x \uplus y) = \#x + \#y - \#(x \cap y) \quad (2.3.1)
\]
does not fit into the induction scheme from Definition 1 since \( \#x \cap \#y \) is not structurally smaller than \( x \uplus y \). Clearly, an alternative induction principle is needed.

A possible solution would be to reason in terms of strict subsets, which would require to show that strict subsets is a well-founded relation. However, it turns out that we can work around this problem by defining an alternative representation of finite sets, equivalent to \( \mathcal{K}(A) \) and more suited for this purpose.

More concretely, we introduce a representation of finite sets based on lists.

Definition 2.7. Given a type \( A \), we define the type \( \mathcal{L}(A) \) of listed finite sets as follows.

Higher Inductive Type \( \mathcal{L}(A) := \)
\[
\begin{align*}
\text{nil} & : \mathcal{L}(A) \\
\text{dupl} & : \prod_{a : A}, \prod_{x : \mathcal{L}(A)} a :: a :: x = a :: x \\
\text{coml} & : \prod_{a, b : A}, \prod_{x : \mathcal{L}(A)} a :: b :: x = b :: a :: x \\
\text{truncl} & : \prod_{x, y : \mathcal{L}(A)} \prod_{p, q : x = y} p = q
\end{align*}
\]

We do not show the induction and recursion principles for \( \mathcal{L}(A) \). What matters here is, that we can establish an equivalence between the representations of finite sets based on Kuratowski sets and lists.

Theorem 2.8. \( \mathcal{K}(A) \cong \mathcal{L}(A) \).

This is proven by constructing a bi-invertible map from \( \mathcal{K}(A) \) to \( \mathcal{L}(A) \) and, assuming the univalence axiom, this equivalence becomes an equality. With the equivalence we derive a new recursion principle for Kuratowski sets.

Proposition 2.9. The type \( \mathcal{K}(A) \) satisfies the primitive recursion principle given in Figure 2.

Proof. Let \( e : \mathcal{K}(A) \rightarrow \mathcal{L}(A) \) be the equivalence defined in Theorem 2.8. By recursion on \( \mathcal{L}(A) \) and using the inverse of \( e \), there exists \( \mu : \mathcal{L}(A) \rightarrow \varphi \). Consequently, the composition \( \mu \circ e \) can be taken as the map \( \text{rec}_{\mathcal{K}(A)}(\ldots) : \mathcal{K}(A) \rightarrow \varphi \) described in Figure 2. \( \Box \)

3 Decidability

Now there is only one obstacle left to define the size function: membership needs to be decidable. Equivalently, we need to define membership as a Boolean predicate in contrast to the previous section’s definition as a proposition.

In addition, in many situations it is convenient to have membership defined as a Boolean predicate. For example,
\[ \varphi : \text{Type} \quad \varnothing \varphi : \varphi \quad \vdash \square \varphi : A \to \mathcal{K}(A) \to \varphi \to \varphi \]

\[ \text{trunc} : \text{ishset}(\varphi) \]

\[ \text{dup} : \prod_{a : A} \prod_{x : \mathcal{K}(A)} \prod_{p : \varphi} \quad \vdash \square \varphi : a \varphi \quad \vdash \square \varphi : a \varphi \]

\[ \text{com} : \prod_{a : A} \prod_{x : \mathcal{K}(A)} \prod_{p : \varphi} \quad \vdash \square \varphi : a \varphi \quad \vdash \square \varphi : a \varphi \]

\[ \text{there exists} \quad \text{rec}_{\mathcal{K}(A)}(\varphi, \ldots, \text{com}) : \mathcal{K}(A) \to \varphi \]

\[ \text{such that} \quad \text{rec}_{\mathcal{K}(A)}(\ldots)(\varnothing) \equiv \square \varphi, \]

\[ \quad \text{rec}_{\mathcal{K}(A)}(\ldots)(a) \cup x \equiv a \varphi \quad \text{rec}_{\mathcal{K}(A)} x \]

**Figure 2.** A primitive recursion principle for \( \mathcal{K}(A) \)

It now makes sense to equip \( \mathcal{K}(A) \) with a lattice structure, we need to define intersection and for that we also need decidable membership.

As we shall see, for defining those operations, some decidability notion for the equality on \( A \) is both sufficient and necessary. More precisely, we show that **decidable mere equality** is suitable for our purpose. Recall that a type \( A \) has decidable mere equality if we have an inhabitant of type \( \prod_{(x, y : A)} |x = y| + |\neg(x = y)| \).

Interestingly enough, even though decidable mere equality might seem innocent, it actually is not. Indeed, it yields the law of excluded middle if it holds in general.

**Theorem 3.1.** If all types have decidable mere equality, then the law of excluded middle holds.

**Proof.** Given \( P : \text{hProp} \), consider the quotient type \( \text{Bool}/\sim \) where \( \sim : \text{Bool} \to \text{Bool} \to \text{hProp} \) is defined by

\[ \text{false} \sim \text{true} \equiv \text{true} \sim \text{false} \equiv \top, \]

\[ \text{false} \sim \text{false} \equiv \text{true} \sim \text{true} \equiv \bot. \]

First, note that \( \sim \) is an equivalence relation. Hence, by [46, Lemma 10.1.8], the type \( [\text{false}] \equiv [\text{true}] \) is isomorphic to \( \top \).

Since all types are assumed to have decidable mere equality, the quotient \( \text{Bool}/\sim \) does so as well. Therefore, we have an inhabitant of type \( |[\text{false}]| = |[\text{true}]| + |\neg([\text{false}]|) = |[\text{true}]| = |[P]| + |\neg[P]| \).

Finally, since \( P \) is a mere proposition, we have \( |[P]| = P \) and thus we have an inhabitant of \( P + \neg P \). Hence, the law of excluded middle holds. \( \square \)

### 3.1 Decidable Membership

To construct a Boolean membership predicate, let us first show that propositional membership is decidable whenever \( A \) has decidable mere equality.

**Proposition 3.2.** For a type \( A \) with decidable mere equality and \( x : \mathcal{K}(A) \) we have an inhabitant

\[ \text{dec} (a \in x) : a \in x + \neg(a \in x). \]

**Proof.** By induction on \( x \), using the fact that \( \text{Empty} \) is decidable and that decidability is closed under +. The assumption is used in the singleton case. \( \square \)

Now we can define the Boolean membership predicate.

**Definition 3.3.** We define \( \epsilon_d : A \to \mathcal{K}(A) \to \text{Bool} \) by case distinction on \( \text{dec} (a \in x) \).

\[ a \in_d x \equiv \begin{cases} \text{true} & \text{if} \ \text{dec} (a \in x) = \text{inl} p \ \text{with} \ p : a \in x; \\ \text{false} & \text{otherwise.} \end{cases} \]

Note that the predicate \( a \in_d \cdot \) meets the expected specification for membership. That is, \( a \in_d \varnothing = \text{false} \) and \( a \in_d x \cup y \) is equal to \( a \in_d x \lor a \in_d y \). Furthermore, \( a \in_d \{a\} = \text{true} \), while \( a \in_d \{b\} = \text{false} \), whenever we have \( \neg(a = b) \). In addition, extensionality holds for \( \epsilon_d \), i.e., assuming for all \( a : A \) the equality \( a \in_d x = a \in_d y \) implies the equality \( x = y \). It turns out that the decidable mere equality on \( A \) is not only sufficient, but also necessary condition for the decidable membership predicate.

**Proposition 3.4.** If the proposition \( a \in x \) is decidable, then \( A \) has decidable mere equality.

**Proof.** Given \( a, b : A \), the type \( a \in \{b\} \) is equal to \( |a = b| \). Since the former is decidable, the latter is as well. Hence, the type \( |a = b| \) is decidable for all \( a \) and \( b \) and thus \( A \) has decidable mere equality. \( \square \)

### 3.2 Size

Now we have all the ingredients to define the size function.

**Proposition 3.5 (Size).** There is a size function on finite sets, denoted by \( \# : \mathcal{K}(A) \to \mathbb{N} \).

**Proof.** We use the primitive recursion principle in Figure 2. The element \( \varnothing \) is mapped to 0. We map \( \{a\} \cup x \to \# x \) if \( a \in_d x = \text{true} \) and to \( \# x + 1 \) otherwise. Now we have two proof obligations left. We briefly indicate how to prove them. First, for \( \text{dup} \) we need to show that \( \#([a] \cup [a] \cup x) \) is equal to \( \#([a] \cup x) \). This follows directly from the two equalities \( a \in_d \{a\} = \text{true} \) and \( a \in_d x \cup y = a \in_d x \lor a \in_d y \). Second, for \( \text{com} \) we need to show that \( \#([a] \cup \{b\} \cup x) \) is equal to \( \#([b] \cup \{a\} \cup x) \). Here we use the decidability of mere equality. We have two cases to consider. If \( |a = b| \), we get \( p : a = b \). Rewriting along \( p \) solves it. Otherwise, we have \( \neg|a = b| \), which gives us \( \neg(a = b) \). Then, \( a \in_d \{b\} = \text{false} \), which, together with the equality \( a \in_d x \cup y = a \in_d x \lor a \in_d y \) allows us to conclude. \( \square \)

Note that, for the size function as well, decidable mere equality on \( A \) is necessary.

**Proposition 3.6.** Given a map \( s : \mathcal{K}(A) \to \mathbb{N} \) such that

1. For \( a : A \) we have \( s \{a\} = 1 \);
2. Whenever \( s x = 1 \), then there merely exists an \( a : A \) such that \( x = \{a\} \).
then the type $A$ has decidable mere equality.

Finally, note that the size function meets its specification, i.e., it verifies the Equation 2.3.1. We do not describe here the proof but instead, we explain how we define the intersection of finite sets, which leads us to another interesting topic, namely how to equip the type $\mathcal{K}(A)$ with a lattice structure.

### 3.3 Lattice Structure

To equip $\mathcal{K}(A)$ with a lattice structure, we need to define a meet operator which, in our case, is intersection. To do so, we introduce the comprehension operation.

**Definition 3.7 (Comprehension).** For $\varphi : A \to \text{ Bool}$ and $x : \mathcal{K}(A)$ we define $\{ x \mid \varphi \}$ by induction on $x$ as follows

$\varnothing \mid \varphi \equiv \varnothing,$

$\{ a \} \mid \varphi \equiv \text{ if } \varphi \text{ then } \{ a \} \text{ else } \varnothing,$

$\{ x \cup y \mid \varphi \equiv \{ x \mid \varphi \} \cup \{ y \mid \varphi \}.}$

For the image of $\text{idem}$ we use Lemma 2.3. For the images of the other path constructors, we can take the corresponding constructor itself in each case.

With this in place, we can define intersection.

**Definition 3.8 (Intersection).** If $A$ has decidable mere equality, then we define $x \cap y \equiv \{ x \mid a, a \in \varnothing \}.$

Note that intersection behaves correctly with respect to the membership predicate.

**Proposition 3.9.** For $a : A$ and $x, y : \mathcal{K}(A)$ we have

$a \in \varnothing \cap y = a \in x \cap a \in y.$

Finally, we equip $\mathcal{K}(A)$ with a lattice structure.

**Theorem 3.10.** The type $\mathcal{K}(A)$ is a lattice with join and meet operations $\cup, \cap,$ and minimal element $\varnothing.$

Let us just illustrate how we prove commutativity for the intersection. Other lattice laws are proved similarly. To show that $x \cap y = y \cap x,$ we start by using extensionality. Then, to show that $a \in \varnothing \cap y = a \in x \cap a \in y$ for all $a : A,$ we use Proposition 3.9, so it suffices to show

$a \in \varnothing \cap a \in \varnothing \cap y = a \in \varnothing \cap a \in \varnothing \cap x.$

This follows from the fact that $\cap$ on Booleans is commutative.

Note that this proof can be automated in Coq. The main ingredient is equipping the Booleans with a lattice structure and then this method can be described with a tactic.

Let us finish this section by showing that, as with decidable membership and size, decidable mere equality on $A$ is necessary for the lattice structure. To this end, we use the following result.

**Proposition 3.11 (Mere Choice).** We have an inhabitant of type $\prod (x : \mathcal{K}(A)), (x = \varnothing) + \prod (a : A), a \in x.$

### 4 Finite Types

In constructive mathematics, there are genuinely different ways of stating that a set has a finite number of elements [20, 44]. A first one would be counting the elements, which leads to the notion of Bishop-finiteness [13, 52]. However, this notion is rather restrictive since, for example, Bishop-finite subsets are not closed under union in general.

Alternatively, one could represent collections with some data type and then use them to enumerate elements of types. Using lists is the most straightforward. However, enumerating a type by lists without truncation would make the notion of finiteness proof-relevant since list equality is too strict. By truncating, it can be made proof-irrelevant again. Nevertheless, by truncation elimination, the list of enumerated elements can be obtained when proving a proposition.

As we shall see, this problem can be overcome by using Kuratowski-finiteness instead since its definition does not involve truncation. Moreover, we shall see that the Kuratowski-finiteness [29] is generally less strict than Bishop-finiteness.

To study the aforementioned finiteness notions, we first need to introduce the notion of subobjects of a given type $A.$ This allows us to define a semi-lattice structure on subobjects of $A$ and to see which notions of finiteness preserve it.

#### 4.1 Subobjects

We first need to recall the definition of subobjects [40, 46].

**Definition 4.1.** Given a type $A,$ we define a type $\text{ Sub}(A)$ by the function type $A \to \text{ nProp.}$ Inhabitants of $\text{ Sub}(A)$ are called subobjects. We say that a function $\lambda x.\|a = x\|$ represents a singleton subobject, which we write as $\langle a \rangle.$ We say that $a$ is a member of $X$ if $X a,$ which we write as $a \in X.$
Intuitively, an inhabitant \( m \) of \( \text{Sub}(A) \) represents a subset of \( A \) by assigning to each element of \( A \) a truth value indicating whether it is a member of \( m \). Note that by extensionality \( \text{Sub}(A) \) is a set since \( h\text{Prop} \) is a set. Moreover, from the lattice structure on \( h\text{Prop} \), we get one for \( \text{Sub}(A) \) by defining the operations \( \lor \) and \( \land \) pointwise.

Before investigating the aforementioned finiteness notions, let us prove the following auxiliary lemma:

**Lemma 4.2.** Given a type \( A \) with decidable equality, \( b : A \), and \( Y : \text{Sub}(A) \) such that \( b \notin Y \), we have

\[
\sum (a : A), a \in (b) \cup Y \simeq (\sum (a : A), a \in Y) + \text{Unit}.
\]

**Proof.** We construct a bi-invertible map. Define \( f \) for \( a : A \) and \( p : a \in (b) \cup Y \) by case distinction on \( \text{dec} (a = b) \).

If \( a = b \), then \( f(a;p) = \text{inr} \text{tt} \).

If \( a \neq b \), then we have \( p = \text{tr} (\text{inr} p') \) and we define \( f(a;p) = \text{inl}(a;p') \).

The inverse \( g \) is defined by \( g(\text{inr}(\text{tt})) = (b; \text{tr}(\text{inl}(\text{tr reﬂ})) \) and \( g(\text{inl}(a;p)) = (a; \text{tr}(\text{inr} p)) \). The assumption \( b \notin Y \) is needed to prove these maps are indeed inverses. \( \square \)

### 4.2 Finite by Counting

Let us start by defining Bishop-finiteness [13, 52].

**Definition 4.3.** For \( n : \mathbb{N} \) we define the standard finite cardinals by \( \emptyset \equiv \text{Empty} \) and \( [n + 1] \equiv [n] + \text{Unit} \).

**Definition 4.4.** A type \( A \) is Bishop-finite, written as \( \text{isBf}(A) \), if there is \( n : \mathbb{N} \) such that \( |A| \simeq [n]| \).

**Definition 4.5.** A subobject \( P : \text{Sub}(A) \) is Bishop-finite, written as \( \text{isBf}(P) \), if \( \sum (x : A), P x \) is Bishop-finite.

Note that \( \text{isBf}(A) \) is a mere proposition. We abbreviate Bishop-finite by \( B\text{-finite} \). The \( B\text{-finite} \) types come together with an induction principle [9] which corresponds to the following lemma.

**Lemma 4.6.** Let \( P : \text{Type} \to h\text{Prop} \) be a family such that \( P \text{ Empty}, \) and \( P(X + \text{Unit}) \) for all \( X : \text{Type} \) with \( \text{isBf}(X) \) and \( P X \). Then we have \( \prod (X : \text{Type}), \text{isBf}(X) \to P X \).

Next we study the structure on \( B\text{-finite} \) types. The empty type is \( B\text{-finite} \), but for singleton subobjects the underlying type needs to be a set. This is both necessary and sufficient.

**Proposition 4.7.** If \( A \) is a set, then all its singleton subobjects are Bishop-finite.

**Proof.** It suffices to show \( \{a\} \) is contractible with center \( (a; \text{tr reﬂ}) \). Let us show that all \( (b; p) \), equal to \( (a; \text{tr reﬂ}) \). Since \( A \) is a set, by truncation recursion we obtain \( q : b = a \) from \( p : |b = a| \). For first coordinate we use \( q \); for the second that \( A \) is a set. \( \square \)

**Proposition 4.8.** If all singleton subobjects of \( A \) are \( B\text{-finite} \), then \( A \) is a set.

Since \( S^1 \) is not a set, we deduce that not every singleton subobject of \( S^1 \) is \( B\text{-finite} \). For example, \( \{\text{base} \} \), for which we have \( S^1 \equiv \{\text{base} \} \), cannot be \( B\text{-finite} \), because then \( S^1 \) would be a set.

Next we look at the union of Bishop-finite subobjects, and here decidable equality is both sufficient and necessary. We first need two lemmas.

**Lemma 4.9.** Given a subobject \( P : \text{Sub}(A) \) and an equivalence \( f : (\sum (a : A), P a) \simeq [n + 1] \), we get

\[
\sum_{P^{\sim} \text{Sub}(A)} \sum_{b : A} (\sum P a = (P' a \lor |a = b|)) \times (\sum P' a \simeq [n]).
\]

**Proof.** For simplicity, we only give the proof in the case where \( A \) is a set. Define a mapping \( P' a := \sum_{y:n} y = \pi_1(f^{-1}(\text{inl} y)) \) and \( b := f^{-1}(\text{inr} \text{tt}) \).

First we show that \( P' a \) is a proposition. Suppose \( \{x_i : p_i \} \) is a set. Then the result follows from the lattice \( h\text{Prop} \). The bi-invertible maps are \( f'(a(y;p)) = y \) and \( g'y = (\pi_1(f^{-1} y); (y; \text{tr reﬂ})) \).

Finally, we show that \( P a = P' a \lor |a = b| \) for all \( a : A \). Since it is an equality between propositions, it suffices to prove a bi-implication. For the implication from right to left, there are two cases.

If \( p : P' a \), then \( P a \) holds since we have \( f^{-1}(\text{inl} (\pi_1 p)) \) and \( \pi_2 p \). Otherwise, \( p : |a = b| \), and then \( P a \) holds because we have \( P b \) by definition.

For the other direction, suppose that we have \( p : P a \). There are two cases to consider. Either \( f(a;p) = \text{inl} y \) for \( y : [n] \) or \( f(a;p) = \text{inr} \text{tt} \). If \( f(a;p) = \text{inl} y \), then \( P' a \) holds by definition of \( P' \). If \( f(a;p) = \text{inr} \text{tt} \), then \( b = \pi_1(f^{-1}(\text{inr} \text{tt})) = \pi_1(f^{-1}(f(a;p))) = a \) \( \square \)

**Lemma 4.10.** If \( A \) has decidable equality, then membership of Bishop-finite subobjects is decidable.

**Proposition 4.11.** If \( A \) has decidable equality, then Bishop-finite subobjects are closed under union.

**Proof.** Given is \( X, Y \subseteq \text{Sub}(A) \) such that both \( X \) and \( Y \) are \( B\text{-finite} \). We use induction on the size \( n \) of \( X \). If \( n = 0 \), then \( X = \emptyset \), and thus \( X \cup Y = Y \) is \( B\text{-finite} \).

If \( n = n' + 1 \), then we use Lemma 4.9 to find \( P' \) and \( b \). Since membership is decidable by Lemma 4.10, there are two cases to consider.

If \( b \in X' \cup Y \), then \( X \cup Y = X' \cup Y \). Then the result follows from the induction hypothesis.

Otherwise, \( b \notin X' \cup Y \), and then there is \( m \) such that \( \sum_{a:A} a \in X' \cup Y \simeq [m] \). We show \( \sum_{a:A} a \in X \cup Y \simeq [m + 1] \).
in three steps.

\[
\sum_{a \in A} a \in X \cup Y \cong \sum_{a \in A} a \in X' \cup Y \lor \left|\left| a = b \right|\right| \\
\cong \left( \sum_{a \in A} a \in X' \cup Y \right) \lor \\text{UNIT} \\
\cong [m] + \\text{UNIT} \cong [m + 1].
\]

The first equivalence follows from Lemma 4.9, and the second step follows from Lemma 4.2. \(\square\)

**Proposition 4.12.** If Bishop-finite subobjects of a set \(A\) are closed under union, then \(A\) has decidable equality.

**Proof.** Let \(a\) and \(b\) be of type \(A\). Since singleton subobjects are Bishop finite, \(\{a\} \cup \{b\}\) is so as well by assumption. Note that we have \(p, q\) such that \((a; p), (b; q) : \{a\} \cup \{b\}\). This means we have \(n\) such that \(\{a\} \cup \{b\} \simeq \{n\}\). Since the goal is a proposition, we obtain \(f : \{a\} \cup \{b\} \to \{n\}\). Now there are three cases: either \(n = 0\), or \(n = 1\), or \(n = n' + 2\).

If \(n = 0\), then we get a contradiction since \(\{a\} \cup \{b\}\) is inhabited by \((a; p)\). If \(n = 1\), then \(\left|\left| a = b \right|\right|\) follows from the fact that \([1]\) is a proposition, and thus

\[a = f^{-1}(f(a; p)), 1 = f^{-1}(f(b; q)), 1 = b.\]

If \(n = n' + 2\), then \([n] = ([n'] + \\text{UNIT}) + \\text{UNIT}\). We show \(-\left|\left| a = b \right|\right|\), so given \(p : a = b\), we get a contradiction. Define \((x_1; p_1) = f^{-1}(\\text{inl}(\\text{inr} \text{tt}))\) and \((x_2; p_2) = f^{-1}(\\text{inr} \text{tt})\) from which we get \(p'_i : \left|\left| x_i = a \right|\right| + \left|\left| x_i = b \right|\right|\) for \(i = 1, 2\) by truncation recursion.

There are several cases to consider depending on the type of \(p'_i\), but in all cases we get \(x_1 = x_2\), so \((x_1; p_1) = (x_2; p_2)\). Since \(f\) is an equivalence, we have \(\\text{inl}(\\text{inr} \text{tt}) = \\text{inr} \text{tt}\) which is a contradiction. \(\square\)

Hence, the Bishop-finite subobjects of \(A\) only possess a join-semilattice structure if \(A\) has decidable equality.

### 4.3 Finite by Enumeration

Alternatively, one can say that an type is finite iff we can enumerate its elements. Such a type is called enumerated in constructive mathematics [44]. If we enumerate the elements by lists, then there are multiple ways to prove some type is finite as various lists can represent the same set. However, with the “logic to type theory” translation [46, Definition 3.7.1], we get a proof-irrelevant version.

**Definition 4.13.** A type \(A\) is enumerated if there is an inhabitant of type \(\text{isEn}(A) := \| \Sigma_{a : A} \\text{member } x \|\) where \(\text{member} : A \to \text{List}(A) \to \text{HProp}\) is the membership predicate on lists.

An alternative way to guarantee proof-irrelevance, is by using the type \(\mathcal{K}(A)\) rather than lists. This gives Kuratowski-finite types [29].

**Definition 4.14.** A type \(A\) is Kuratowski-finite if there is a term of type \(\text{isKf}(A) := \Sigma (X : \mathcal{K}(A)), \| (a : A), a \in X \|\).

**Proposition 4.15.** The type \(\text{isKf}(X)\) is a mere proposition.

**Proof.** Define \(\varphi X := \prod_{a : A} a \in X\). By [46, Chapter 2.7] it suffices to show that \(\varphi X\) is a proposition and that \(X = Y\) whenever \(\varphi X\) and \(\varphi Y\).

By function extensionality, \(\varphi X\) is a mere proposition. If \(\varphi X\) and \(\varphi Y\), then by Theorem 2.5 we get \(X = Y\). \(\square\)

These notions coincide as shown by the following two propositions. Their proofs are straightforward.

**Proposition 4.16.** Enumerated types are Kuratowski-finite.

**Proof.** Define a map \(f : \text{List} A \to \mathcal{K}(A)\) by \(f \text{ nil} = \varnothing \land f(a \mathbin{::} l) = \{a\} \cup f l\). Then we have \(\text{member } a l = a \in f l\). For any enumerated type \(A\), we have a witness \(l : \text{List} A\) proving its finiteness since isKf is a proposition. Then \(f l\) proves \(A\) is Kuratowski-finite. \(\square\)

**Proposition 4.17.** Kuratowski-finite types are enumerated.

**Sketch.** The recursion principle from Figure 2 can also be translated into an induction principle in the usual fashion. With that, we show

\[
\prod_{x : \mathcal{K}(A)} \prod_{l : \text{List}(A)} \prod_{a : A} a \in x = \text{member } a l ||. 
\]

Since truncations are propositions, it suffices to provide images for the point constructors. If \(x = \varnothing\), we pick \(\text{tr}(\text{nil}; \lambda a \text{ refl})\). Otherwise, \(x = \{a\} \cup x'\). We have the induction hypothesis

\[
H : \| \Sigma_{l : \text{List} A} \prod_{a : A} a \in x' = \text{member } a l ||. 
\]

This gives us \(l' : \text{List}(A)\) and \(p : \prod_{a : A} a \in x' = \text{member } a l'\) by truncation recursion. Then the desired inhabitant is

\[
\text{tr}(a : l' ; \lambda b \text{ ap} (\lambda z. ||b = a|| \lor z) (p b)). \quad \square
\]

In addition, we can talk about Kuratowski-finite subobjects for which we first map \(\mathcal{K}(A)\) into \(\text{Sub}(A)\). For that we define a map fset by \(\lambda (X : \mathcal{K}(A)) (a : A), a \in X\). Let us first show that different finite sets represent different subobjects.

**Proposition 4.18.** The map fset is an embedding.

**Proof.** By the results [46, Section 4.6], it suffices to show that fset is injective, because both \(\text{Sub}(A)\) and \(\mathcal{K}(A)\) are sets. Assuming fset \(X = \text{fset } Y\), we obtain the proof of \(\prod (a : A), (a \in X = a \in Y)\) by definition of fset. Then \(X = Y\) follows from Theorem 2.5. \(\square\)

**Definition 4.19.** A subobject \(P : \text{Sub}(A)\) is Kuratowski-finite if \(\sum_{X : \mathcal{K}(A)} P = \text{fset } X\).

We abbreviate Kuratowski-finite by K-finite. Let us now move to the structure of K-finite subsets. The first example is \(S^1\), which shows that being a set is not necessary.

**Example 4.20.** The circle \(S^1\) is Kuratowski-finite.
Proof. Take \( X = \{ \text{base} \} \). We show \( \prod_{x: \text{base}} x = \{ \text{base} \} \) by induction on \( \text{S}^1 \). For base we take \( \text{tr}(\text{refl}) : || \text{base} = \text{base} || \), and for loop we use that \( ||x = \text{base}|| \) is an \( \text{HProp} \). \( \square \)

Furthermore, unlike B-finiteness, singleton subobjects are always K-finite subobjects and K-finite subobjects are closed under union. In addition, they are closed under surjections, products, and sums.

**Theorem 4.21.** K-finite types are closed under surjections, products and sums. Singletons are K-finite subobjects. K-finite subobjects are closed under union.

To prove that K-finiteness is preserved under products, we make a map \( \cdot \times \cdot : \mathcal{K}(A) \to \mathcal{K}(B) \to \mathcal{K}(A \times B) \) such that \( a \in X \times Y \iff a \in X \) and \( a \in Y \). Now, if \( A_1 \) and \( A_2 \) are K-finite, we can find \( X_1 : \mathcal{K}(A_1) \) and then \( X_1 \times X_2 \) witnesses the finiteness \( A_1 \times A_2 \). For the other statements, we use the same technique.

Let us finish this section by comparing B-finiteness and K-finiteness. In general, the former is stronger than the latter.

**Proposition 4.22.** Bishop-finite types are Kuratowski-finite.

Proof. Let \( A \) be a Bishop-finite type. We prove the statement \( \text{isKf}(A) \) by Bishop-finite induction (Lemma 4.6), using the fact that \( \text{isKf}(A) \) is a proposition (Proposition 4.15). The requirements follow from Theorem 4.21. \( \square \)

Since B-finite types are sets ([52, Proposition 2.4.8]), this notion is strictly stronger than K-finiteness by Example 4.20. However, they coincide if the type has decidable equality.

**Theorem 4.23.** If \( A \) has decidable equality, then \( A \) is B-finite iff it is K-finite. Consequently, a type is B-finite iff it is K-finite and it has decidable equality.

Proof. The direction from left to right corresponds to Proposition 4.22. For the other direction, we use \( \mathcal{K}(A) \)-induction to establish \( \exists X : \mathcal{K}(A) \), \( \text{isBF}(\text{set} X) \). Since \( \text{isBF} \) is a proposition, it suffices to provide images for the point constructors. If \( X = \emptyset \), then \( \text{set} \emptyset \) is Bishop-finite since we have \( \{0\} \cong \{x : A \mid \text{Empty} \} \). The other cases follow from Lemma 4.7 and Proposition 4.11. \( \square \)

## 5 Interface for Finite Sets

To obtain sound programs which use finite sets, one first models sets by either list-like or tree-like data structures. Then one writes programs and specifications and finally one proves properties that relate the programs and specifications. Implementing this in a proof assistant requires a significant number of properties about operations of the data structure which are proven directly on the implementation level.

Since list-like and tree-like structures can be seen as concrete representations of finite sets, modeling them explicitly as such might be useful in the development process. Indeed, this would allow one to reason about correctness of programs on the abstract level of finite sets where various lattice laws and other properties hold “on the nose” rather than via the induced equivalence on the concrete implementation (a so-called “setoid equality”). Moreover, a function defined on the abstract representation, can be refined into a function defined on any given implementation, and functions on a concrete representation can be transferred to another.

We start this section by discussing how we can use our definition \( \mathcal{K}(A) \) of finite sets for this approach and then illustrate it on a small example.

### 5.1 Method

Consider a type operator \( T : \text{Type} \to \text{Type} \). Intuitively, \( T \) is an implementation of \( \mathcal{K}(A) \) if for all \( A : \text{Type} \) there exists an interpretation function \( \llbracket \cdot \rrbracket_T \) from \( T(A) \) to \( \mathcal{K}(A) \) providing structure-preserving implementations of the three point constructors and propositional membership. For this, we use the definitions of signatures, interpretations and homomorphisms, which are translated from model theory. Formally, we have the following definitions.

**Definition 5.1** (Interpretation). Let \( \Sigma_A \) be a type. Denote by \( \Sigma_A \) the signature with a nullary symbol \( \emptyset \), a binary symbol \( \cdot \cup \cdot \), and for each \( a : A \), a nullary symbol \( \{a\} \) and a unary predicate \( a \in \cdot \).

A type \( B \) is an interpretation of \( \Sigma_A \) if there is \( \emptyset_B : B \), an operation \( \cup_B : B \to B \to B \), and if for each \( a : A \) there is \( \{a\}_B : B \) and a predicate \( a \in_B \cdot : B \to \text{HProp} \).

Given two interpretations \( T \) and \( S \) of \( \Sigma_A \), a map \( f \) from \( T \) to \( S \) is a homomorphism if

\[
\begin{align*}
  f(\emptyset) &= \emptyset_S & f(x \cup y) &= f(x) \cup_S f(y) \\
  f(a) &= a_S & a \in_T x &= a \in_S f(x)
\end{align*}
\]

Note that \( \mathcal{K}(A) \) itself is an interpretation of \( \Sigma_A \) and thus we can talk about homomorphisms into \( \mathcal{K}(A) \).

**Definition 5.2.** A type operator \( T : \text{Type} \to \text{Type} \) is an implementation of finite sets if for each \( A \) the type \( T(A) \) is an interpretation of \( \Sigma_A \) and for each \( A \) we have a homomorphism \( \llbracket \cdot \rrbracket_T \) from \( T(A) \) to \( \mathcal{K}(A) \).

Suppose now that we are given an implementation \( T \) of finite sets. First, note that the predicate \( a \in_T \cdot \) behaves as expected, i.e., we have for all \( a \in A \),

\[
\begin{align*}
  (a \in_T \emptyset) &= (a \in \emptyset) = \\text{Empty}, \\
  (a \in_T \{b\}) &= ||a = b||, \\
  (a \in_T x \cup_T y) &= (a \in_T x \lor a \in_T y).
\end{align*}
\]

Next, let us show that \( \llbracket \cdot \rrbracket_T \) is a surjective homomorphism.

**Proposition 5.3.** The map \( \llbracket \cdot \rrbracket_T : T(A) \to \mathcal{K}(A) \) is surjective.

Proof. To show that \( \llbracket \cdot \rrbracket_T : T(A) \to \mathcal{K}(A) \) is surjective, we need to prove \( \llbracket \cdot \rrbracket_T : T(A) \to \mathcal{K}(A) \) is surjective. We use induction on \( \mathcal{K}(A) \). Since being surjective is a mere proposition, we only need to consider the point constructors.
Finite Sets in Homotopy Type Theory

For \( Y = \emptyset \) and \( Y = \{a\} \), we use \( \emptyset_T \) and \( \{a\}_T \) respectively. For \( Y = Y_1 \cup Y_2 \) we assume \( p_i : \prod X_i : T(A) \), \( [X_i]_T = Y_i \) for \( i = 1, 2 \) and we need to find an inhabitant of the mere proposition \( \prod X_i : T(A), [X_i]_T = Y_i \). With truncation recursion we get \( X_i : T(A) \) and \( q_i : [X_i]_T = Y_i \) from \( p_i \). From the \( q_i \) we get a path \( q \) of type \( [X_1 \cup X_2]/\sim_T = [X_1]/\sim_T \cup [X_2]/\sim_T = Y_1 \cup Y_2 \) and for the desired inhabitant we choose \( \text{tr}(X_1 \cup X_2, q) \). □

In general, \( T(A) \) might have fewer equalities than \( \mathcal{K}(A) \), so we cannot guarantee the map \( [\cdot]_T \) is injective. Nevertheless, it always induces an equivalence relation on \( T(A) \) by defining \( x \sim_T y \) iff \( [x]_T = [y]_T \). Moreover, using the fact that \( [\cdot]_T \) is a homomorphism, we can conclude that the types \( x \sim_T y \) and \( [\cdot](a : A) \), \( a \in_T x = a \in_T y \) are equivalent.

Furthermore, we factor the map \( [\cdot]_T \) using the quotient type \( T(A)/\sim_T \) according to the diagram below

\[
\begin{array}{ccc}
T(A) & \xrightarrow{[\cdot]_T} & \mathcal{K}(A) \\
\downarrow & & \downarrow \phi_T \\
T(A)/\sim_T & \xrightarrow{m_T} & \mathcal{K}(A)/\sim_T
\end{array}
\]

where the map \( m_T \) is constructed by recursion on the quotient type \( T(A)/\sim_T \). Before proceeding, let us show that the quotient type \( T(A)/\sim_T \) and \( \mathcal{K}(A) \) are indeed equivalent.

**Proposition 5.4.** The map \( m_T \) is an equivalence.

**Proof.** Following Theorem 4.6.3 of [46], it suffices to show that \( m_T \) is both an embedding and a surjection.

To show that \( m_T \) is an embedding, it suffices to show \( m_T \) is an injection since \( T(A)/\sim_T \) and \( \mathcal{K}(A) \) are sets. Let \( x_1, x_2 \) be two arbitrary elements of \( T(A)/\sim_T \). We use the recursion on both \( x_1 \) and \( x_2 \). Since quotient types are sets, it suffices to look at the points. So, we need to show that \( x_1 \sim_T x_2 \) whenever \( [x_1]_T = [x_2]_T \), which follows by definition.

The surjectivity of \( m_T \) follows from Proposition 5.3 since whenever \( y = [x]_T \), we have \( y = [x]_T = m_T [x] \). □

Note that even though \( T(A) \) might not be a semi-lattice, the quotient type \( T(A)/\sim_T \) is always one. Indeed, we can reflect the semi-lattice structure from \( \mathcal{K}(A) \) using the equivalence \( m_T \). Doing so guarantees that \( [\cdot] \) becomes a homomorphism.

Even if we are just interested in the implementation \( T(A) \), this is still useful, because equalities in the quotient can be reflected to the relation \( \sim_T \) we defined.

**Proposition 5.5.** We have \( [x] = [y] \iff [x]_T = [y]_T \).

Last, but not least, given a function from a certain implementation of finite sets to some type \( B \), we can get that function from another implementation to \( B \).

**Theorem 5.6.** Suppose, we are given two implementations \( T \) and \( S \) of finite sets. Then from a map \( f : T(A) \to B \) respecting \( \sim_T \), we get a map \( S(A) \to B \).

**Proof.** This follows from the diagram

\[
\begin{array}{ccc}
S(A)/\sim_T & \xrightarrow{m_S} & \mathcal{K}(A) \to T(A)/\sim_T \\
\downarrow & \xrightarrow{m_T} & \downarrow h \\
S(A) & \to B
\end{array}
\]

where \( h : T(A)/\sim_T \to B \) is obtained by quotient-type recursion from \( f \) and the fact that \( f \) respects \( \sim_T \). The map \( S(A) \to B \) is obtained by composition in the diagram. □

Since \( \mathcal{K}(A) \) itself is an implementation of finite sets, we immediately gain the following corollary.

**Corollary 5.7.** Given an implementation \( T \) of finite sets and a map \( \mathcal{K}(A) \to B \), we get a map \( T(A) \to B \).

5.2 Application

Let us illustrate our method on the example of lists. We define interpretation of \( \Sigma_A \) for \( \text{List}(A) \) as follows

\[
\text{List}(A) \equiv \text{nil}, \quad \{a\}_\text{List}(A) \equiv a :: \text{nil},
\]

\[
\cup_{\text{List}(A)} \equiv \text{append}, \quad \in_{\text{List}(A)} \equiv \text{member}.
\]

We define a homomorphism \( [\cdot] : \text{List}(A) \to \mathcal{K}(A) \) by

\[
[nil] \equiv \emptyset, \quad [x :: xs] \equiv \{x\} \cup [xs].
\]

Consequently, we get \( l_1 \sim l_2 \) iff for all \( a \) : \( A \) we have member \( a \) : \( l_1 \) = member \( a \) : \( l_2 \).

The fact that \( \text{List}(A)/\sim \) is a semi-lattice implies that the induced append operation is commutative even though the append operation is not. From Proposition 5.5 we get that append \( x \) \( y \) and append \( y \) \( x \) have the same elements. This way we can for example prove that \( l \) and reverse \( l \) have the same elements.

Finally, assuming that \( A \) has decidable mere equality, we transfer the size function (Proposition 3.5) from \( \mathcal{K}(A) \) to \( \text{List}(A) \). This means that we make the map \( \#_L : \text{List}(A) \to \mathbb{N} \) according to Corollary 5.7. By working out the definitions, we get

\[
\#_L \text{ nil} = 0,
\]

\[
\#_L (a :: l) = \text{if} \ \text{member} \ a \ l \ \text{then} \ \#_L \ l \ \text{else} \ \#_L \ l + 1.
\]

The same way we can define bounded quantification for lists. Both quantifiers exist and for all are done similarly, so we only show forall here. Let us start by defining it on \( \mathcal{K}(A) \) and showing it has the right specification.

**Definition 5.8.** We define the universal quantifier forall of type \( (A \to \text{Prop}) \to \mathcal{K}(A) \to \text{Prop} \) by induction on \( \mathcal{K}(A) \). For the point constructors we define

\[
\forall \phi \emptyset \equiv \text{Unit},
\]

\[
\forall \phi \{a\} \equiv \phi \ a,
\]

\[
\forall \phi (x :: y) \equiv (\forall \phi \ x) \times (\forall \phi \ y).
\]

For the paths we need to prove that \( (\text{Prop}, \times, \text{Unit}) \) is a semi-lattice which is straightforward.
Proposition 5.9. The operation forall meets the following specification representing the introduction and elimination rule of universal quantification

\[ \forall I : \prod_{x : \mathcal{K}(A)} \left( \prod_{a : A} a \in x \rightarrow \varphi a \right) \rightarrow \text{forall} \varphi x, \]

\[ \forall E : \prod_{x : \mathcal{K}(A)} \left( \prod_{a : A} \text{forall} \varphi x \rightarrow a \in x \rightarrow \varphi a \right). \]

Using Definition 5.8 and Corollary 5.7 we define a quantifier forall : \((A \rightarrow \text{hProp}) \rightarrow \text{List}(A) \rightarrow \text{hProp}\) on lists. The specifications in Proposition 5.9 can be translated to List(A) and the quantifier forall\_satisfies these.

6 Related Work

There have been several proposals to describe the syntax and semantics of HITs in general [2, 7, 8, 18, 36, 42]. HITs originating from these schemata can be implemented in Coq [9], Agda [15], and Lean [17, 26, 49].

Furthermore, several constructive interpretations of fragments of homotopy type theory exist. The operational semantics of a small fragment of univalence is given, capturing extensionality in higher order propositional logic [1]. Both the groupoid model [22, 23] and 2-dimensional type theory [34] are constructive, but only model a fragment of homotopy type theory (groupoids). Cubical sets and cubical type theory give a model with inductive types and numerous examples of non-trivial higher inductive types combined with univalence at all levels [11, 16]. However, a constructive interpretation of HoTT including all higher inductive types remains to be given.

Higher inductive types have been applied to numerous problems in computer science including partiality [3, 47], homotopical patch theory [6], type theory formalized in type theory [4, 5], and even real numbers [21]. In addition, HITs have been used to define spaces in synthetic algebraic topology of which the homotopy is studied [24, 32, 33, 35, 46].

Bounded quantification has also been defined for enumerated sets [19]. In addition, the authors showed that bounded quantification of decidable properties is again decidable. The same results hold for our notion of finite sets.

In constructive mathematics finiteness has extensively been studied [13, 44, 50] and Kuratowski finite sets have been studied both in a classical [29] and constructive setting [14, 25]. Other definitions include Bishop-finiteness [13], enumerated sets [44], streamless sets, and Noetherian sets [12, 20, 37–39, 44]. The latter three notions have also been translated to type theory [10, 19, 48], but only in a proof-relevant fashion i.e., without truncation. Note also that streamlessness and Noetherianness both are weaker than enumeratedness, which we studied in Section 4.

The finite sets defined by Firsov et al. and Parmann always have decidable equality [19, 38, 39], but there also are variations of Noetherianness which do not imply decidable equality [20]. In contrast, Kuratowski-finiteness does not imply decidable equality and we systematically use the weaker notion of decidable mere equality.

Furthermore, hereditary finite sets were studied in type theory for which categoricity and consistency were shown by Smolka et al. [41]. In their work, the definition of a hereditary finite structure — a model for hereditary finite sets — is similar to Definition 2.7. In addition, since the structures are defined axiomatically, this gives an interface for finite sets.

In homotopy type theory, it has been proven that the universe of sets forms a predicative topos [40, 46] and Bishop finiteness has been implemented [51, 52], although neither of those consider Kuratowski-finite sets.

Other interfaces of finite sets have been developed, most notably by Krebbers and Wiedijk in the CH2O formalization of the C-standard [28] and by Lescuyer [31]. In contrast to our work, those developments use setoids instead of higher inductive types. The usage of higher inductive types allows us to avoid considerations regarding well-definedness of the maps, as all defined functions automatically respect equality.

7 Conclusion and Perspectives

Higher inductive types offer a flexible method to work with finiteness. Using HITs, we can define a data type of finite sets \( \mathcal{K}(A) \) for which reasoning is sufficiently simple and which has the right level of abstraction. In addition, using the data type \( \mathcal{K}(A) \) we define finite subobjects, finite types and an interface for finite sets.

In constructive mathematics there is still an amount of theory about Kuratowski finite sets left untouched in our development [14, 25]. Some work has already been done to prove that the decidable Kuratowski-finite sets form a topos in Theorem 4.21, but for a full proof, function spaces and the subobject classifier have to be considered as well.

In a similar fashion to Definition 2.1, we can define bags. This would allows us to define when two lists represent the same bag i.e., when two lists are permutations of each other. A sorting algorithm would then be defined by a map sort from lists to ordered list such that \( l \) and sort \( l \) represent the same bag. This technique could simplify correctness proofs of sorting algorithms. Furthermore, since these two definitions are similar, it would be interesting to see whether techniques from "data types à la carte" would be applicable [45].

In Coq, there already are several implementations and interfaces of finite sets. One of them is included in the Coq distribution [30]. It requires giving several operations satisfying some specifications and it is more expanded than our interface. The specifications for operations present in our interface can be derived. However, a complete connection between the two would require additional work.

To make the developed material work best, a computational interpretation of the univalence axiom and higher inductive types is needed since that would allow actually
Finite Sets in Homotopy Type Theory

executing the code. Steps have been made towards this goal especially in cubical type theory [1, 11, 16], but a computational interpretation of higher inductive types is still missing.

Acknowledgments
The authors thank the anonymous reviewers of the HoTT/UF workshop, Guillaume Allais and Cory Knapp for useful tips. The authors would also like to thank the CPP reviewers for their careful reading and comments on the paper.

The first three authors were supported by the STW project 14319, which is (partly) financed by the Netherlands Organisation for Scientific Research (NWO).

References
[32] Daniel R Licata and Guillaume Brunerie. 2013. $\pi_n(S^0)$ in Homotopy Type Theory. In International Conference on Certified Programs and


